Goddard Procedures and Guidelines

DIRECTIVE NO.	GPG 2810.1	**APPROVED BY Signature:**	*Original Signed by*
EFFECTIVE DATE:	April 16, 2003	**NAME:**	A. V. Diaz
EXPIRATION DATE:	April 16, 2008	**TITLE:**	Director

Responsible Office: 100/Office of the Director

Title: Security of Information Technology

TABLE OF CONTENTS

PREFACE

P.1 PURPOSE

This Goddard Procedures and Guidelines (GPG) establishes policies, procedures and responsibilities for assuring appropriate levels of availability, confidentiality and integrity for Goddard Space Flight Center (GSFC) information technology (IT) resources and constitutes the GSFC Information Technology Security (ITS) Program.

P.2 APPLICABILITY

a. The NASA applicability of this document can be found in NPG 2810.1, paragraph 1.3.

b. This GPG applies to all GSFC employees and GSFC contracts (as provided by the terms and conditions of the contract), where appropriate in achieving Center missions, programs, projects, and institutional requirements. GSFC includes the Wallops Flight Facility (WFF), Goddard Institute for Space Studies (GISS), Independent Validation & Verification Facility (IVV), and the White Sands Space Complex (WSC).

c. Readers should note that this GPG applies only to the security of unclassified automated information, applications, and computer and telecommunications systems. The processing of classified automated information and secure telecommunications is the responsibility of the GSFC Security Branch (Code 205.1).

P.3 AUTHORITY

a. NPD 2800.1, Managing Information Technology
b. NPD 2810.1, Security of Information Technology
c. NPG 2800.1, Managing Information Technology
d. NPG 2810.1, Security of Information Technology

P.4 REFERENCES

a. NPD 1382.17, Privacy Act – Internal NASA Direction in Furtherance of NASA Regulations
b. NPD 1440.6, NASA Records Management
c. NPD 1600.2, NASA Security Policy
d. NPD 1620.2, NASA Badging System
e. NPD 7120.4, Program/Project Management
f. NPD 9800.1, NASA Office of Inspector General Programs
g. NPG 1441.1, NASA Records Retention Schedules
h. NPG 1620.1, Security Procedures and Guidelines
i. NPG 7120.5, NASA Program and Project Management Processes and Requirements

P.5 CANCELLATION

a. GMI 2410.6, Assuring Security and Integrity of the GSFC Automated Information Resources
b. GHB 1600.1, Goddard Security Manual, Chapter 18
c. Center Interim Guidance for Information Technology Security dated March 5, 1998

P.6 SAFETY

None.

P.7 TRAINING

None.

P.8 RECORDS

Record Title	Record Custodian	Retention
IT System Security Plan	Center IT Security Manager	*NRRS 2/14B2 Destroy when active reference value ceases or when 3 years old, whichever is later.
Authorization to Process Information	Center IT Security Manager	*NRRS 2/12B22 Destroy when 8 years old.
Security Review Document	Center IT Security Manager	*NRRS 2/14B2
NASA Baseline IT Security Requirement Waiver	Center IT Security Manager	*NRRS 2/12B22
Center Firewall Rules Waiver	Chair, Center Firewall Review Board	*NRRS 2/12B22
Account Request Document	Center IT Security Manager	*NRRS 2/12B22

**NRRS – NASA Records Retention Schedules (NPG 1441.1)*

P.9 METRICS

The goal of the IT Security Planning process is to achieve an appropriate level of security in IT systems. The NASA Metrics to track this are found in NPG 2810.1, paragraph 3.1. Additionally the center will track the following metric:

All users of Government-owned or -funded IT resources complete Agency-required IT Security training.

P.10 DEFINITIONS

a. Application data backup/recovery - Data backup is the process of saving software and information on magnetic media and storing the media in a location away from the IT facility. This process provides the means to ensure application recovery, that is, the means to restore the application/information after damage to or destruction of the IT hardware, software, or information.

b. Audit/review - The survey of an IT system to evaluate the adequacy of implemented controls, assure they are functioning properly, identify vulnerabilities, and assist in implementation of new controls where required. This survey is conducted annually, or whenever significant change has occurred, for all IT systems and may lead to recertification of the IT system.

c. Automated logon sequences - A computer program or script that performs user connection to IT without user intervention after initiation.

d. Chain letter - An electronic mail note that either explicitly or implicitly encourages the user to forward the note to multiple recipients with no discernible end to the chain or no specific benefit to the Government for doing so.

e. Civil service line managers - Center management officials who are responsible and accountable for assuring the integrity, availability, and confidentiality of sensitive/critical data, applications, systems and networks in their organizations.

f. Compliance-based - A structured, top-down approach to IT security wherein each system must meet the same standards set program wide.

g. Console logon - Accessing IT from the computer operator's system control console. Console logons are generally granted privileged-user status.

h. Console logs:
   (1) Important system events that are recorded and printed at the system control console.
   (2) Handwritten journals of important events kept by the computer operator.

i. Continuity of operations - The steps taken by the civil service line manager to assure that reasonable data processing support can be provided should events occur that prevent normal operations.

j. Controlled access area - An area where access is physically limited to authorized personnel. Access may be controlled by various methods such as guards, cipher locks, electronic badge readers, etc.

k. Data custodian - An individual designated by the data owner to have the responsibility for making judgments and decisions on behalf of the organization with regard to the data's information category designation, its use and protection, and the sharing of that data.

l. Decrypt - To render encrypted information intelligible by affecting a series of transformations through the use of variable elements controlled by the application of a key to the given representation of the information. Also see Encrypt.

m. Digital signature - An authentication tool that verifies the origin of a message and the identity of the sender and receiver.

n. Directorate - Codes 110, 150, 200, 300, 400, 500, 600, 800, 900 and 100 (includes all organizations in Code 100).

o. Domain name system - A database system that translates an IP address into a domain name.

p. Environmentally controlled area - An area where temperature and humidity can be controlled to the extent that magnetic media and specialized equipment can be stored without damage.

q. External label - For the purpose of GPG 2810.1, physical labels placed on the outside of magnetic media that identify their contents.

r. Failed logon - Any unsuccessful attempt to gain user access to IT resources.

s. Foreign national - A citizen of any country other than the United States.

t. GSFC Information Technology Security Program - The program documented and described in the current edition of GPG 2810.1.

u. Hard copy output - Paper or film output from an IT system, such as line printer output, printed console logs, paper plots, microfiche, etc.

v. Independent review - A review of any GSFC IT system conducted by person(s) not associated with that particular system. Such a review may be conducted at any time at the option of the Center Director, CIO, or ITSM.

w. Internal label - Header blocks on magnetic media that identify their contents.

x. IT security controls - The physical, electronic, and administrative IT security measures established and applied to IT facilities and IT hardware, firmware, software, and information that afford the appropriate level of protection to ensure integrity, availability, and confidentiality.

y. Magnetic media – Media, such as magnetic tapes and disks, that stores data.

z. Malicious intruder - An individual who intentionally gains access to a computer without authorization. Malicious intruders may be insiders or outsiders.

aa. Management Control Processes - The established methods and procedures that assure that the requirements for a Center-level IT security program are implemented in a manner consistent with the current edition of GPG 2810.1.

bb. Media library - An environmentally controlled area for the storage of magnetic media, such as magnetic tapes and disks.

cc. NASA IT Security Clause – NASA FAR Supplement Clause 1852.204-76, implements the contractual requirements for safeguarding the integrity of unclassified NASA IT systems and data. The clause is applicable to any contract where IT resources (e.g., data, information, applications, and systems), are integrated into and support the NASA missions, whether the contractor is a commercial entity or a university.

dd. Organization - Any functional group of employees for which a permanent manager has been appointed.

ee. Privileged user - Any local user who is not the appointed system administrator but who has been granted administrator, root or privileged-user operating system rights on any computing device.

ff. Residual risk - For the IT system manager, the risk that remains when all other known risks have been either mitigated to the maximum extent possible or fully corrected.

gg. Risk value - The probability that any given threat will occur, multiplied by the impact of the concomitant loss.

hh. Risk-based - An approach to IT security intended to place the decisions on what risks, and how much risk to accept, in the hands of civil service line managers who are most familiar with the environment in which they have to operate.

ii. Special Management Attention System - An IT system that requires special attention to security due to the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of information in the system. Loss of a Special Management Attention System would have a major, and in some cases catastrophic, impact on the Agency's mission.

CHAPTER 1 - Information Technology (IT) Security Roles and Responsibilities

All GSFC employees who manage, use, program, or operate GSFC IT resources, as well as contracts under which GSFC IT resources are provided or are affected, have responsibilities for ensuring that appropriate levels of integrity, availability, and confidentiality are maintained throughout the life cycles of these systems. The purpose of this chapter is to define GSFC civil service positions having such responsibilities.

1.1 Center Management and Key IT Security Roles

1.1.1 The Center Director

The Center Director has overall responsibility for the GSFC ITS Program. The Center Director responsibilities are stated in NPG 2810.1, paragraph 2.2.1.

One additional Center-specific responsibility is to appoint a Chief Information Officer (CIO) to whom responsibility for the Center ITS Program is delegated.

1.1.2 Chief Information Officer (CIO)

The responsibilities of the CIO are stated in NPG 2810.1, paragraph 2.2.2.

Additional Center-specific responsibilities are:

a. Coordinating and advocating of information management policies that directly support the missions at GSFC as well as those of the Agency.
b. Establishing yearly productivity objectives that are verifiable and measurable for information system services and security.
c. Assisting the ITSM in developing information security policies and standards for all information, including safeguards for protecting the accumulation, preservation and dissemination of information.
d. Ensuring that programs and procedures are in place to reduce or eliminate the vulnerability of communications networks ands computers to disruption and damage.
e. Establishing and maintaining the GSFC information infrastructure architecture and ensuring continual compliance with NASA policy and procedures.
f. Ensuring that sufficient resources are budgeted and available to implement and maintain the technical security controls of the Center's IT infrastructure.
g. Ensuring that the NASA Incident Response Center (NASIRC) complies with NASA CIO requirements.
h. Chairing the Information Technology Federation Board (ITFB).
i. Approving equivalent training for NASA required IT Security training.
j. Charter the Center's Computer Security Officials Working Group.

1.1.3 Center Information Technology Security Manager (ITSM)

The responsibilities of the Center IT Security Manager are stated in NPG 2810.1, paragraph 2.2.4.

Additional Center-specific responsibilities are:

a. Reporting to the CIO the status of the ITS program.
b. Providing metrics and reports on the ITS Program, as required, to the NASA Competency Center for ITS (NCCITS).
c. Notifying the Center Incident Response Team about IT Security incidents.
d. Chairing the Center Computer Security Official's Working Group (CSOWG).
e. The ITSM will promptly (within the first 2 hours of the next workday) notify the CIO of IT security incidents.

1.1.4 Information Technology Federation Board (ITFB)

The ITFB is responsible for:

a. Reviewing Center IT Security policies.
b. Making recommendations to the CIO on IT Security policies.

1.1.5 Goddard Network Engineering Configuration Control Board

A representative from the Information Services and Advanced Technology (ISAT) Division chairs the Goddard Network Engineering Configuration Control Board (GNECCB). The GNECCB is comprised of standing members and ex-officio members. Standing members are permanently assigned to the Board and will participate in all Board decisions. The purpose of the GNECCB is to review technical proposals and maintain strategic direction of institutional networks in accordance with the Center Network Strategic Plan and appropriate Agency and Center standards.

1.2 Center Support Roles

1.2.1 Chief Financial Officer

The Chief Financial Officer is responsible for the security of financial, accounting, and asset management systems.

1.2.2 Chief, Procurement Operations Division

The responsibilities of the Chief, Procurement Operations Division are stated in NPG 2810.1, paragraph 2.3.4.

An additional Center-specific responsibility is to ensure compliance with the Electronic Freedom of Information Act Amendments of 1996 and applicable laws, in coordination with the Center Chief Counsel.

1.2.3 Chief, Information Services and Advanced Technology (ISAT) Division

The Chief, Information Services and Advanced Technology Division, is responsible for:

a. Ensuring the development of Center wide IT Security policies and guidance.
b. Maintaining a Center intrusion-detection capability.
c. Appointing a chair for the GNECCB.
d. Operating a Center incident response and handling capability.

1.2.4 Office of Human Resources

The responsibilities of the Office of Human Resources training office are stated in NPG 2810.1, paragraph 2.3.2.

Additional Center-specific responsibilities are:

a. Appointing an IT Security Awareness Training Coordinator.
b. Ensuring that each new employee (civil service) receives IT Security awareness training prior to being turned over to his or her supervisor.
c. Ensuring that each employee newly assigned to a management position successfully completes IT Security for Managers within 30 days of his or her new assignment.

1.2.5 Center Chief of Security (Head, Security Branch)

The responsibilities of the Center Chief of Security are stated in NPG 2810.1, paragraph 2.3.1.

Additional Center-specific responsibilities are:

a. Issuing Center IT standards, best practices, and guidance to protect command and control data during uplink transmission.
b. Issuing Public Key Infrastructure (PKI) certificates as the Center Registration Authority (RA).

1.2.6 The Center Export Administrator

The Center Export Administrator (CEA) is responsible for ensuring the compliance of all Center program activities with U.S. export control laws and regulations.

1.2.7 IT Security Incident Response Team

The responsibilities of the IT Security Incident Response Team are stated in NPG 2810.1, paragraph 2.3.3.

1.2.8 Center Information Processing Service Organization - Center Network Environment (CNE)

The responsibilities of the Center Network Environment are stated in NPG 2810.1, paragraph 2.2.9.

1.2.9 CSO Working Group

The Center CSOWG is chaired by the ITSM with the Deputy ITSM as vice chair. The working group membership consists of the Directorate Computer Security Officials (DCSOs), Organization CSOs, and their alternates. The CSOWG serves as an advisory body to the ITSM on all matters involving IT Security.

1.3 Organizational Roles

1.3.1 The Director of Each Directorate

The responsibilities of the Director of each directorate are stated in NPG 2810.1, paragraph 2.2.3.

Additional Center-specific responsibilities are:

a. Appropriately identifying all restricted or protected information managed by the Directorate, ensuring that required security controls are in place, and restricting access to authorized persons only.
b. Ensuring that IT Security responsibilities are integrated into individual position descriptions and the annual performance plans of the CSOs.
c. Ensuring that directorate employees complete Agency-required IT security awareness training.
d. Appoint a Directorate Computer Security Engineer (DCSE).

1.3.2 Organizational (Directorate) Computer Security Official (DCSO)

The responsibilities of the Directorate Computer Security Official are stated in NPG 2810.1, paragraph 2.2.6.

Additional Center-specific responsibilities are:

a. Communicating all appropriate IT Security information to the CSOs within their directorate.
b. Ensuring that all information in directorate systems is properly categorized (e.g., SEB, ITAR, EAR, Privacy Act, mission, proprietary) and assigned to the proper information category.
c. Ensuring that all directorate IT resources are included in an IT Security Plan.
d. Implementing a risk management process for all systems and networks in the Directorate.
e. Approve Center Firewall Port Waiver Requests.

1.3.3 Directorate Computer Security Engineer

a. Serving as the advisor to Directorate Management and the DCSO on IT security issues.
b. Oversee the technical aspects of the IT security organization within the directorate.

c. Serving as a member of Center-level committees and boards on IT security led by the Enterprise IT Security Branch.
d. Provide guidance to the system administrators on IT security issues.

1.3.4 Line Manager (Civil Service Line Manager)

The responsibilities of the line manager are stated in NPG 2810.1, paragraph 2.2.7.

Additional Center-specific responsibilities are:

a. Ensuring that ITS responsibilities are integrated into individual position descriptions and the annual performance plan of the CSO and the alternate CSO.
b. Assigning an information category for each system and network in the organization.
c. Authorizing in writing, consistent with center and agency policies, Government employees who may use each system and network that processes or stores Government information.
d. Establishing a security perimeter (e. g., firewalls, routers) between Government-owned or -funded networks and networks external to the Center.
e. Establishing restrictions and controls to prevent networked nodes from having simultaneous connections (back doors) with Government networks and networks external to the Center.
f. Ensuring that only authorized individuals access export control information (e.g., ITAR and EAR).
g. Establishing rules-of-behavior for each system and network and providing them to system and network users.
h. Establishing access controls for physical access into rooms where IT resources are located.
i. Approving all external connections to a Government-owned or -funded network.
j. Ensuring that magnetic media in IT resources designated for excess or transfer are cleared in accordance with the requirements of this GPG.
k. Ensuring that employees complete Agency-required IT security awareness training.

1.3.5 Organizational CSO

The responsibilities of the Organizational CSO are stated in NPG 2810.1, paragraph 2.2.6.

Additional Center-specific responsibilities are:

a. Implementing a risk management process for all systems and networks in the organization.
b. Implementing a process for providing contingency planning and reasonable continuity of operations for systems, networks, and applications in the organization.
c. Identifying and maintaining a list of all systems and networks in the organization.
d. Identifying and maintaining a list of organization network and system administrators.

1.3.6 System Administrator (SA)

The responsibilities of the System Administrator are stated in NPG 2810.1, paragraph 2.2.8.

Additional Center-specific responsibilities are:

a. Promptly installing vendor-issued security-related operating system patches.
b. Maintaining an inventory of system hardware, software and system applications.
c. Granting accounts only to individuals who have been approved by the civil service line manager.
d. Maintaining a file of approved Account Request Documents.

1.4 User Roles

1.4.1 Program and Project Managers

The responsibilities of Program and Project Managers are stated in NPG 2810.1, paragraph 2.4.1.

1.4.2 System and Data Owners

The responsibilities of the System and Data Owners are stated in NPG 2810.1, paragraph 2.4.2.

1.4.3 User Community

The responsibilities of the User Community are stated in NPG 2810.1, paragraph 2.4.3.

CHAPTER 2 – Center Information Technology (IT) Security Program

Chapter 2 discusses the elements of the Center IT Security Program itself and how it is implemented, what kinds of analyses, reviews, and evaluations may be performed, and generally establishes the management tools by which the Center IT Security Program is conducted. This chapter will also describe the elements by which the program is assessed and will relate these program elements back to their governing Federal directives.

2.1 Components of IT Security

IT Security has three components, integrity, availability and confidentiality. These components are discussed in NPG 2810.1, paragraph 1.1.

2.2 Goals and Objectives of the Center IT Security Program

a. The goal of the Center IT Security Program is to ensure that appropriate, cost-effective levels of integrity, availability, and confidentiality are applied to the protection of all of the Center's sensitive unclassified information and systems that support the Center's missions, programs, and functions. The Center IT Security Program implements current Federal law and NASA directives.

b. To accomplish this goal, the Center Director has established the following objectives for the Center IT Security Program. The ITSM is assigned policy and compliance responsibility for the IT Security program.

(1) To assure that all IT systems in the GSFC community have a plan for achieving and maintaining an appropriate, cost-effective level of security which is based on a proactive life-cycle, risk-based approach to IT Security, including planning for contingency operations.

(2) To assure that all individuals who have privileged access are identified in accordance with the sensitivity of information or type of access they require such that an appropriate personnel screening may be accomplished.

(3) To assure that all personnel in the GSFC community, both civil service and contractor, understand their individual responsibilities through appropriate IT Security awareness and training programs.

(4) To assure that effective incident response and reporting processes exist and that all personnel know how to use them.

(5) To assure that appropriate metrics are collected and reported in order to permit management to gauge the effectiveness of the program.

2.3 The Elements of the Center IT Security Program

The elements of the Center IT Security Program are:

a. Assignment of Security Responsibility: Every Special Management Attention (SMA) System and General Support System (GSS) will have security responsibility assigned to an individual knowledgeable of the nature of the information processed and who is competent to apply and manage appropriate security controls.

b. Development of an IT Security Plan: The security of every SMA system and GSS will be documented in an IT Security Plan. Adequate security must be planned for as a normal part of the Center's IT management processes. Planning must include certain areas such as rules for use of the system, requirements for specialized training, personnel and technical controls, and provisions for contingency operations. Detailed information on how to prepare this plan can be found in NPG 2810.1, paragraph 5.1.

c. Independent Periodic Review of Security Controls: The security controls of each SMA system and GSS must be reviewed at least every 3 years or upon significant modification to the system whichever occurs first. The scope and frequency of reviews should be commensurate with the acceptable level of risk for the system in question.

d. Authorization to Process: An appropriate civil service line manager must authorize in writing the use of each SMA system and GSS based upon the implementation of that system's security plan before processing is permitted. Processing must be reauthorized at least every 3 years or upon significant change to the system, whichever occurs first. It is extremely important to note that when the civil service line manager signs this certification he or she is accepting responsibility for the level of risk inherent in operating the IT system.

e. IT Security Awareness and Training: Training is a required part of the security planning process. All individuals who access information in an IT system operated by or on behalf of the Federal Government shall be trained commensurate with their responsibilities. Readers will find guidance for IT Security awareness and training in Chapter 4.

f. Personnel Screening: Personnel screening is a required part of the security planning process. Every individual who is granted privileged access to system and controls must be screened consistent with the risk or harm that could be caused. It is not a requirement for other users to be investigated. Readers will find guidance in Chapter 4 for identifying and reporting the names of individuals who are required to be screened as part of the process for granting them access.

g. Incident Response: Within the scope of their duties, all users of IT systems must be able to recognize an incident, respond to it appropriately, and report it to proper authorities. Readers will find guidance in Chapter 4 for recognizing, responding to, and reporting IT security incidents.

2.4 A Risk-Based Versus a Compliance-Based IT Security Program

Generally speaking, computer security programs are of two types: compliance-based and risk-based. The compliance-based approach is highly structured and depends upon a set of rules, issued by an appropriate Government or corporate authority and mandatory for all participants in the program.

Compliance-based programs provide a common set of security goals for the participants but leave the least flexibility to the individual system managers who are accountable for the successful operation of the system. A risk-based security program, on the other hand, places the burden directly upon civil service line managers to discern and understand their risks and then make reasonable decisions about what risks to accept versus what risks to mitigate or correct. NASA has implemented a risk-based program.

2.5 IT Security management at the Center Level

a. Periodic review, evaluation, and the reporting of IT security activities are fundamental requirements in the management control of the Center's IT Security Program. Reports on any aspect of the program are issued upon the request of NASA CIO, the Center CIO, or the Center Director.

b. The ITSM is the primary point of contact for release of information regarding the Center's IT security posture to other Government Agencies and to organizations outside the Government. All such reports will be coordinated with NASA Headquarters, the Center director, the CIO and the Office of Public Affairs, as appropriate except as otherwise provided under NASA regulations implementing the Freedom of Information Act and other provisions concerning release of information.

CHAPTER 3 – Information Technology (IT) Security Requirements

The Federal government has established certain mandatory IT security requirements for the protection and processing of IT resources. This chapter discusses these requirements and the procedure for requesting a waiver.

3.1 Federal IT Security Requirements

3.1.1 Waiverable Versus Nonwaiverable Requirements

No one within the NASA community can waive Federal requirements for IT security. These requirements are embodied in the Public Laws of the United States or promulgated by other directives of the Federal Government. The nonwaiverable Federal requirements are stated in NPG 2810.1, paragraph A.5.1.

3.2 NASA Baseline IT Security Requirements

a. The NASA Baseline IT Security requirements are technical, administrative, and physical security requirements that result from interpretation of Federal and Agency directives. A civil service line manager may accept the risk of not implementing some of these provisions, if it is documented and receives the concurrence of the ITSM, CIO, or Center Director.

b. The NASA Baseline IT Security Requirements are found in NPG 2810.1, Appendix A.

c. Any NASA baseline IT Security Requirement that is not met must be documented in the IT Security Plan.

3.3 Waiver of IT Security Requirements

Civil service line managers may not always be able to meet the technical requirements in the NASA Baseline IT Security Requirements. The procedure for submitting a waiver of an IT Security requirement is discussed in NPG 2810.1, paragraph A.5.

CHAPTER 4 – Center IT Security Requirements and Procedures

This chapter identifies Center IT Security requirements and provides guidance on various matters of regulation, policy and ethics that are of concern to users of Center IT resources.

4.1 Center Requirements

4.1.1 Required IT Security Documentation

4.1.1.1 IT Security Plan – (see NPG 2810.1, paragraph 5.1 for format)

Each system is required to be covered by an approved IT Security Plan. The IT Security Plan is the single published source that describes how security for a particular IT system will be conducted. The risk assessment must be incorporated into the IT Security Plan. The risk assessment documents the risks of the risk assessment, the risk-reduction analysis, the risk mitigation actions that have been taken and the risks that civil service line management has agreed to accept. The IT Security Plan (including the risk assessment) must be reviewed every 3 years. Civil service line management is responsible for assuring the completion and signing of the IT Security Plan. See NPG 2810.1, paragraph 4.2 for the NASA guidelines for IT security planning. A Center-developed template for the IT Security Plan can be found at http://forbin2.gsfc.NASA.gov/297/docs/doc-templates.stm.

4.1.1.2 IT Security Contingency Plan – (See NPG 2810.1, paragraph 5.3 for format)

The IT Security Contingency Plan describes the arrangements that have been made and the steps that will be taken to continue system operations in the event of a natural or human-caused disaster. The contingency plan must meet the requirements of NPG 2810.1, must be reviewed and tested periodically (annually or upon significant change) and must be signed by civil service line management. A Center-developed template for the IT Contingency Plan can be found at http://forbin2.gsfc.nasa.gov/297/docs/doc-templates.stm.

4.1.1.3 System Rules of Behavior

The System Rules of Behavior (required by OMB Circular A-130, Appendix III) describes the rules that users of the system must adhere to. These rules should clearly delineate responsibilities/expected behavior of all individuals who use the system. It must be in writing and distributed to each user of the system. The Center developed format for the System Rules of Behavior can be found at http://forbin2.gsfc.NASA.gov/297/docs/doc-templates.stm.

4.1.1.4 Authorization to Process

The Authorization to Process (required by NPG 2810.1, paragraph 4.2.12.1) is management's declaration that they are satisfied with the security controls in place and that they accept the risk to operating the system. Civil service line management must authorize each system to process before

operation of the system. This authorization must be in writing and must be renewed every 3 years or upon significant change. The Center developed format for the Authorization to Process can be found at http://forbin2.gsfc.NASA.gov/297/docs/doc-templates.stm.

4.1.1.5 Assignment of Responsibility

a. Directorate CSO/Organizational CSO:

(1) Each Directorate must appoint a Directorate CSO to oversee the security of IT resources that are the responsibility of the Directorate. This person must be a civil servant and the appointment must be in writing. A copy of the appointment letter must be provided to the ITSM.

(2) Each organization within the Directorate must appoint a CSO who is responsible for the security of all IT resources within the organization. The CSO must be a civil servant and the appointment must be in writing designating the individual. A copy of the appointment letter must be provided to the ITSM. The alternate CSO may be civil servant or contractor, provided that, for contractor CSOs, the CSO requirement is properly documented in the pertinent contract's statement of work or task order, that the contractor and not a civil servant designates the individual to perform such function, and that the contractor employee is not subject to supervision by civil servants. Contractor designation of personnel shall be in accordance with applicable contract provisions, but need not be in writing unless required by the contract.

b. System Administrator - Each system must have a system administrator responsible for the security of the system. The system administrator may be civil servant or contractor provided that for contractor designations, the provisions referenced in a. (2) above for designation of contractor alternate CSOs are followed. This assignment must be in writing and provided to the ITSM. Contractor designation of personnel shall be in accordance with applicable contract provisions and provided to the ITSM by the contract's COTR.

c. System Administrator - Each system must have a system administrator responsible for the security of the system. The system administrator may be civil servant or contractor. This assignment must be made in writing. A copy of the appointment letter must be provided to the ITSM.

4.1.2 IT Security Awareness and Training

a. The NASA procedures for IT Security Awareness and Training are covered in NPG 2810.1, paragraph 4.3.

b. All NASA required IT Security training is available as Web-based training hosted at https://solar.msfc.NASA.gov:443/solar/delivery/public/html/newindex.htm.

c. Equivalent training approved by the Center CIO may be substituted for NASA-required IT security training.

4.2 Center Procedures

4.2.1 Granting Access

Center practice continues to be one of giving civil service line managers the authority and responsibility to grant access to IT resources under their control as their needs dictate. Procedures for granting access can be found in NPG 2810.1, paragraph 4.7.

4.2.2 Procedure for Granting IT Access

The procedure for system administrators to grant IT access (US citizens and foreign nationals) can be found in NPG 2810.1, paragraph 4.7.7. A center developed template for the Account Request Document that complies with the requirements in NPG 2810.1, paragraph 4.7.7 can be found in Appendix G.

4.2.3 IT Security Incident Reporting and Handling

4.2.3.1 IT Security Incident Defined

An IT security incident is defined in NPG 2810.1, section 4.4.2.1.

4.2.3.2 Incident Categories

The NASA incident categories can be found in NPG 2810.1, section 4.4.11.

4.2.3.3 Reporting an IT Security Incident

a. The Center procedure for reporting IT security incidents can be found in Appendix D.

b. The ITSM's responsibilities for reporting IT security incidents can be found in NPG 2810.1, paragraph 4.4.4.

4.2.3.4 Remediation Process for Compromised Systems

Computer systems that have suffered a root compromise are disconnected from all Center networks. The actions that must be completed before they can be reconnected are stated in Appendix C.

4.2.3.5 Center Incident Notification Alert Roster

a. The purpose of this Alert Roster is to provide a Center point of contact list for responding to serious IT Security incidents requiring immediate attention. A serious IT security incident is (1) A system (root) compromise, (2) hacked Web page, (3) denial of service attack, or (4) widespread virus infection not detected by anti-virus software. The current Center Incident Notification Alert roster can be found at http://forbin2.gsfc.nasa.gov/297/report-inc_compromise.stm.

b. The objective is to minimize further damage and the impact that a serious IT security incident can cause.

c. The individuals listed on the alert roster are responsible for appropriately and promptly addressing these incidents.

d. During normal duty hours, appropriately and promptly addressed means:

(1) Identifying the responsible SA;
(2) Notifying the DCSO and others on the alert roster;
(3) Evaluating the severity of the compromise (impact) to the compromised system and its information, the likelihood of further hostile activity against the compromised system or other systems;
(4) Determining a course of action, i.e., a risk-based decision to remove system from the local network and Internet or maintain system on network for mission purposes; and
(5) Documenting actions taken, personnel contacted, and time spent, and cost of other resources utilized.

e. After hours, appropriately and promptly addressed means:

(1) Evaluating the severity of the compromise (impact) to the compromised system and its information, the likelihood of further hostile activity against the compromised system or other systems;
(2) Deciding whether or not to remove the system from the local network and Internet access based upon the impact and as much information as can be readily obtained (within 1-2 hours) by contacting the "data owners" and managers who may be familiar with the system (if possible), by attempting to contact the SA, and talking with others on the alert roster;
(3) Documenting actions taken, personnel contacted, time spent, and cost of other resources utilized; and
(4) Contacting the DCSO and SA the next business day.

4.2.3.6 GSFC IT Security Incident Review Board

The Center IT Security Review Board was established to review serious IT security incidents that result in a root compromise. Only the CIO, Head, Enterprise IT Security Branch, OIG Computer Technology Crimes Office and the ITSM are authorized to request the convening of the Center IT Security Review Board. The Board will decide if the actions taken to correct the conditions that caused the incident are sufficient to warrant reconnection to a Center network.

a. Membership

*Chair - CIO
*Vice chair - ITSM/Deputy ITSM
*Center Incident Response Team representative
*NASIRC project manager
*Goddard IT Security Vulnerability Scan Team (GITSVST)

*CNE IT security manager
*HECN ITS representative
*EbNet ITS representative
*HSTNet ITS representative
*IONet ITS representative
Enterprise IT Security Branch representative
OIG Computer and Technology Crimes Office (CTCO) representative, (as required)

* Voting Members

b. Attendees - to be determined by the Incident Organization:

Directorate CSO
Organization CSO
System administrator
Civil service line management
Contractor project management
Others as incident organization deems appropriate

c. Criteria for Convening an IT Security Review Board

(1) Recurring IT security incident(s) (as defined in section 4.2.5.1) on the same host
(2) Request by Computer and Technology Crimes Office (CTCO) due to criminal implications of the incident
(3) More than 1 host compromised by same hostile IP address (if requested by CIO, ITSM or more Senior Center or NASA Management)
(4) Severity of incident (invoked only by CIO or ITSM)

d. Responsibilities

(1) CIO chairs the IT Security Review Board
(2) ITSM/Deputy ITSM:
- Chairs the IT Security Review Board in the absence of the CIO
- Notifies the DCSO and CSO of requirement to appear before the review board
- Schedules the review board in coordination with the DCSO/CSO
- Notifies the review board members
- Notifies the appropriate network security manager to reconnect the system

(3) DCSO
- Request the ITSM to schedule the review board
- Provides the location for the review board

(4) CSO
- Informs civil service line management of the requirement to appear before the review board
- Notifying the appropriate Government COTR about the need for contractor attendance at the review board
- Ensures that all actions required by the Center compromise procedures are completed before requesting convening of the review board
- Gives presentation on actions completed to the review board
- Submits updated IT Security Plan/Authorization to Process/copy of warning banner/ISS vulnerability scan report to the ITSM

(5) Civil service line management ensures that a presentation covering actions completed in remediation of the compromise is prepared.

e. The CSO should include the following subjects in the presentation to the review board:

(1) Remediation work completed to comply with the Center ITS Incident Remediation Process
(2) Actions completed to significantly reduce or fully eliminate the current threat to overall Center IT security
(3) Actions completed on the Center compromise checklist
(4) Training completed for system administrators, system users, and civil service line managers

4.2.4 Permissible Uses of Government IT Systems

a. Official and personal use policies of Government IT Systems are covered in NPG 2810.1, paragraph 4.8. Personal use, consistent with these policies, shall be subject to supervisory approval; supervisors may authorize their own personal use. In addition, the Goddard Connect System (Government-provided dialup access) may be used only for official Government business and may not be used for personal reasons.

4.2.4.1 Ownership of Information in Center-Owned IT Systems

The Notification of Rights to IT Resources can be found in NPG 2810.1, paragraph 4.10.3.

4.2.4.2 Monitoring Computer Systems Operated by or on Behalf of the Center

The monitoring of IT resources operated by or on behalf of the Center is covered in NPG 2810.1, paragraph 4.10.4.

4.2.4.3 Privileges and Limitations of User Access

All users must understand clearly the privileges and limitations of their access to Center systems. Each user's supervisor, sponsor, or system manager can answer these questions.

4.2.5 Software Usage

The requirements and responsibilities for software usage is found in NPG 2810.1, paragraph 4.9.

4.2.6 Notification to Users at Logon

a. The notification to users at logon (warning banner) is covered in NPG 2810.1, paragraph 4.10.2.

b. Warning banners must be displayed on all interactive access points (for example, console login, telnet, ftp, http) and on all non-interactive access points that provide a human readable response (for example, the UNIX operation "finger").

c. In the event that electronic banners and warnings are not supported by a system, printed banners should be used that are clearly visible to the user as they use the system. The following logon banners are for use on all web sites maintained by Goddard.

(For Nonpublic Resource with External Connections)
(Internet Connections)

This U.S. Government resource is for authorized use only.
If not authorized to access this resource, disconnect now.
Unauthorized use of, or access to, this resource may
subject you to disciplinary action or criminal prosecution.
By accessing and using this resource, you are consenting to
monitoring, keystroke recording, or auditing.

(Web Page with Connections to the Internet)
(Public Web Page/Anonymous FTP)

U.S. Government Public Information Exchange Resource
You have accessed a U.S. Government Resource.
This site is intended to be used by the public for information exchange.
Any attempt to modify or exploit this resource or associated information
other than for instructed use is strictly prohibited and may be punishable
under the Computer Fraud and Abuse Act of 1986.
The Government may monitor and audit the usage of this resource.
All persons are hereby notified that use of this resource constitutes consent
for monitoring, keystroke recording, or auditing.

4.2.7 Penetration Testing

The NASA procedures for conducting penetration testing are covered in NPG 2810.1, paragraph 4.6.

4.2.8 Privileged Access or Access with Limited Privileges to Information in Center IT Systems

Privileged access to a computer for the purpose of system administration does not automatically convey rights to examine the information in the files that are administered, even though the administrator's privileges may permit that level of access. For example, a post office server administrator is not necessarily entitled to read the user's mail. System administrators must clearly understand the privileges and limitations of their access. The civil service line manager is responsible for determining the privileged users' boundaries and ensuring that those who exercise privileged access understand and abide by the limits.

4.2.9 Guidelines for Conducting Computer Searches

Goddard officials will cooperate with representatives of the NASA OIG concerning searches.

If non-NASA law enforcement officials request or demand a search, and such official is not accompanied by, or authorized by, a representative of the NASA OIG to conduct such search, any Goddard employee receiving such request shall immediately notify the ITSM before allowing the search. The ITSM will review the search authorization, and shall consult with the Office of Chief Counsel regarding all non-federal search authorizations, prior to authorization of such search. Goddard officials shall allow such searches only with the prior authorization of the ITSM or a representative of the NASA OIG.

For all non-OIG, internal searches, Goddard officials identified under NPG 2810.1, Section 4.10.4.2, (not including NASA OIG representatives) shall conduct such searches only after notification of the ITSM, who will in turn notify the Center CIO, and only after receipt of acknowledgement of the search by the ITSM. Except where an emergency precludes such notification, the Goddard official shall provide a written notice to the ITSM containing the following:

-Identification of the assets to be searched, including, but not limited to, NASA property tag number, Internet Protocol or domain Name Server address, name of individual to whom the asset is assigned, general description of the asset and any associated equipment to be searched, building and room number or other site where located, and any other unique definition.

- Name and position of the official requesting the search
- The extent of the proposed search
- The reasons for the search including the information upon which the need for a search has been determined

The ITSM shall consult with appropriate Goddard officials, including but not limited to the CIO, the Office of Chief Counsel, the Office of Human Resources, and/or the appropriate contracting officer, before acknowledging the search. The ITSM shall specify any conditions, which are to be followed in conducting the search, to include determination that the ITSM shall conduct the search.

4.2.10 Policy on File Transfer Protocol (FTP)

4.2.10.1 General

a. There are two different types of FTP. Anonymous FTP is designed for public release of information. There is no user authentication built in to the anonymous FTP protocol. Authenticated FTP requires the use of passwords and account names to authenticate the users of the service. Unfortunately, these passwords are transmitted in the clear over the network.

b. The use of TCP wrappers restricts access of the FTP service to certain network addresses from which transfer requests are anticipated. The fundamental concept is to match the security level of the systems that are requesting files. By definition, systems located on subnets that can be accessed by anyone on the Internet are less secure than systems located on subnets that can only be accessed by trusted NASA locations. In the event that a compromise occurs for a system open to the Internet, it is necessary to ensure that the compromised system cannot request files from more secure systems.

4.2.10.2 Anonymous FTP

Anonymous FTP connectivity is allowed if the following conditions are met:

a. The data to be accessed has been reviewed and approved for public release or other methods are used to protect nonpublic data (e.g., using nonbrowseable directory structures).
b. A valid IT Security Plan exists for the system on which FTP is to be provided.
c. The system on which the FTP is processed must be scanned prior to connectivity. All high and medium vulnerabilities must be corrected.
d. The system does not have public-read/public-write directories.

4.2.10.3 Authenticated FTP

Authenticated FTP connectivity is allowed if the following conditions are met:

a. The access to the service is restricted by the use of TCP Wrappers, or equivalent methods that restrict access by IP address.
b. A valid IT Security Plan exists for the system on which the FTP service is run.
c. Appropriate logging by the FTP service is turned on.
d. The system providing FTP service must be scanned prior to connectivity. All high and medium vulnerabilities must be corrected.

4.2.11 Policy on the Distribution of System and Network Diagrams

4.2.11.1 Restrictions on Distribution

a. The distribution of Center system or networks diagrams is restricted to those individuals who have demonstrated a need to know the information or where otherwise required by law or regulation. Only those portions of the network diagram that is required for the individual's task will be distributed.

b. System and network diagrams may not be posted on publicly accessible web pages or made available via anonymous FTP unless required by law or regulation.

4.2.12 Mail Relay

4.2.12.1 General

a. Third party mail relay occurs when a mail server allows an external mail client to forward mail to it for processing and delivery. An external mail client is one that is outside of the Center. If an e-mail server allows third party relay, anyone on the Internet can send e-mail messages to the server and it does all the work to parse and deliver the messages. In addition, the mail appears to come from the mail server's site and not from the site that actually sent the message.

b. Third party relay is abused by Internet spammers who use it to send large amounts of spam e-mail (unsolicited commercial mail is the Internet version of junk mail) at the mail server owner's expense. Intruders use it to embarrass a site by spamming with an embarrassing message such as a pornographic letter or advertisement. Intruders also use it to harass some other site by sending thousands of e-mail messages to that other site.

4.2.12.2 Requirement

All Center mail servers having mail relay enabled are required to comply with the Center policy on mail relay service registration. The policy is defined in Appendix F.

4.2.13 Vulnerability Scanning

4.2.13.1 General

NASA has obtained an Agency site license for Internet Security Scanner (ISS). This ISS license permits scanning of any IP address within the nasa.gov domain. Periodic vulnerability scanning will continue to be an important part of the Center IT Security Program for the foreseeable future.

4.2.13.2 Center-Conducted Scanning

a. All NASA required scanning would be conducted using the Agency-mandated scanning tool. Directorate and organization CSO's are provided the results of these scans. Vulnerabilities detected during these scans are required to be corrected within the next fiscal quarter.

b. All computers connecting to a Government-owned or -funded network must be scanned prior to connection. All vulnerabilities detected during the scan must be corrected or obtain an approved waiver before connection. The organization owning the IT resource is responsible for obtaining the waiver**.**

c. The scanning of any IP address outside of the gsfc.nasa.gov domain may be conducted only with the written approval of the CIO or the ITSM.

d. Ad hoc scans are conducted as new vulnerabilities are identified or when requested by NASA Headquarters. The Enterprise IT Security Branch (Code 297) conducts these scans. These scans are announced by Center-wide notice sent to the Directorate and organization CSO's. The following information will be included in this notice.

(1) Purpose of the scan
(2) Authorizing official
(3) The point of contact for information
(4) Schedule for the scan
(5) Target systems
(6) Source IP addresses of the scan
(7) Vulnerability being scanned for
(8) Scanning tool(s) to be used

A follow-up notice will be issued announcing the completion of the scan.

4.2.13.3 Organization Conducted Scanning

The CSO must obtain approval from the CSO's management and DCSO prior to conducting scanning, and may only scan IP addresses that are included within the CSO's direct area of responsibility. Scanning any other IP addresses requires the written approval of the organization responsible for those IP addresses. CSO's must notify the system administrators and users of the systems that a scan will be conducted prior to starting the scan.

4.2.13.4 Requesting an ISS Key

a. The Deputy ITSM is the Center contact to obtain ISS keys. All requests for keys must be made in writing (mail, hand delivered, faxed or encrypted e-mail) with a copy to the ITSM.

b. Three working days should be allowed for processing each request. The DCSO must approve all requests for ISS keys. Each request shall include the following information: (1) Contact information for the person requesting the key. (2) Source IP address of the scan. (3) Target IP addresses to be scanned. (4) Beginning and ending date/time of the scanning. If requester has a PGP key on the NASA HQ server, the keys will be sent to them by PGP encrypted e-mail. If the requester has a PKI certificate the keys will be returned via PKI encrypted e-mail. Otherwise, the CSO will be notified to pick up the diskette containing the ISS key(s).

4.2.14 Use of Standards Ports

a. The use of nonstandard ports greatly complicates Network Management and the response to security incidents. The use of nonstandard ports can be used to circumvent the restrictions imposed by the Center CNE firewall.

b. The Center policy is that the standard ports be used to provide network services. These ports are sometimes referred to as well-known ports.

c. The CIO must approve any request for use of nonstandard ports prior to implementation. The CIO will consider approving the use of nonstandard ports if proprietary software is using normally unassigned ports (usually high-numbered ports) for special purposes, and the software has no provisions for being configured to use standard ports.

4.2.15 Removing Data and Licensed Software From Computer Data Storage Devices Prior to Disposal of IT Resources

a. Federal agencies are required to ensure the security and privacy of Federal information processing resources. Failure to remove sensitive, Privacy Act, proprietary, classified, or mission-critical data and licensed software before transferring or disposing of information technology equipment can lead to the disclosure of sensitive information, copyright violations, costly investigations, and other negative consequences.

b. The Center policy is that data and licensed software be removed from computer data storage devices (commonly referred to as hard disks) prior to transferring control to the Property Disposal Officer.

c. This policy applies to all personal computers (PCs), both IBM-compatible and Macintosh, in Goddard's inventory.

d. All Government-owned and Government-furnished IT equipment must have its magnetic media cleared of all data and licensed software before it is excessed for internal or external transfer, donation, or sale.

e. PCs, which are to be transferred, donated or sold, should have an installed operating system unless the computer was purchased without an operating system.

f. Damaged hard drives will be removed and destroyed.

g. Disposition of Federal records must be accomplished in accordance with 36 Code of Federal Regulations, Chapter XII, Part B and the NASA Records Retention Schedules.

h. Responsibilities

(1) The Property Disposal Officer is responsible for ensuring that PCs received for disposal is certified that the hard drives have been cleared as required by Center policy.
(2) The Information System Branch is responsible for:
  (a) Cleaning data from hard disks of PCs sent to the Property Disposal Officer.
  (b) Verifying that such data cannot be recovered.
  (c) Attaching a certifying sticker to each PC before transferring control to the Property Disposal Officer.
  (d) Installing an operating system.

(3) The civil service line organization owning the property is responsible for:
   (a) Reviewing data on hard drives, identifying Federal records, and either copying (electronically to another medium or storage device or printing a hard copy) or transferring the data to another responsible official (another program official or a records management official).
   (b) Attaching the signed certification statement to the turn-in document, NASA Form 1602, prior to forwarding to the Property Disposal Officer.

4.2.16 Connection of Non-Government Computers

Civil service line management must approve the connection of non-Government computers to IP addresses under their control. The following actions must be completed before the computers can be connected.

a. The computer must be scanned using ISS.
b. All high and medium vulnerabilities must be corrected before it may be connected.
c. The users of non-Government computers must complete the SOLAR course Basic ITS Awareness available at https://solar.msfc.nasa.gov/solar/delivery/public/html/newindex.htm.

4.2.17 Waiver of Center Firewall Rules

a. Organization personnel who feel they have valid justification for leaving a port open may submit a typed Port Waiver Request Form to the DCSO for that organization. The DCSO submits the signed request to the ITSM who brings the request before the CNE Firewall Review Board (CFRB) at the next meeting.

b. Waiver requests may be submitted for review electronically to cfrb-request@listserv.gsfc.nasa.gov. Approved waiver requests will not be implemented until the signed copy is received.

c. The CFRB meets weekly to approve/disapprove requests and, if necessary, gathers additional information from the technical point of contact (T-POC) listed on the request. Both the T-POC and the DCSO will be kept updated as to the status and informed when a decision has been reached.

d. The current status of CNE Firewall ports closure can be found at http://cne.gsfc.NASA.gov/security/portblocking.htm.

e. Changes to the CNE Firewall Rule Set are implemented at the end of each workday.

Appendix A – Acronyms and Abbreviations

	A
ADM	Administrative
ATP	Authorization to Process
	B
BRT	Business and Restricted Technology
	C
CA	Certificate Authority
CCS	Center Chief of Security
CEA	Center Export Administrator
CIO	Chief Information Officer
CNE	Center Network Environment
COMSEC	Communication Security
COTR	Contracting Officer's Technical Representative
COTS	Commercial off-the-shelf
CSO	Computer Security Official
CSOWG	Computer Security Official Working Group
CTCO	Computer and Technology Crimes Office
	D
DCSO	Directorate Computer Security Official
DCSE	Directorate Computer Security Engineer
	E
EAR	Export Administration Regulation
EBnet	EOS Backbone network
EO	Executive Order
	F
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
	G
GHB	Goddard Handbook
GISS	Goddard Institute for Space Studies
GITSVST	GSFC IT Security Vulnerability Scan Team
GMI	Goddard Management Instruction
GNECCB	Goddard Network Environment Configuration Control Board
GPG	GSFC Procedures and Guidelines
GSFC	Goddard Space Flight Center
GSS	General Support System
	H
HECN	High Energy Computing Network
HQS	NASA Headquarters
HST	Hubble Space Telescope

I

ID	Identifier
IOnet	IP Operational Network
IP	Internet Protocol
ISAT	Information Services and Advanced Technology Division
ISS	Internet Security Scanner
IT	Information Technology
ITAR	International Traffic In Arms Regulations
ITFB	Information Technology Federation Board
ITS	Information Technology Security
ITSM	Information Technology Security Manager
IVV	Independent Validation & Verification Facility

L

LAN	Local Area Network

M

MSN	Mission

N

NA	Network Analyzer
NAC	National Agency Check
NASA	National Aeronautics and Space Administration
NASIRC	NASA Incident Response Center
NIST	National Institute of Standards and Technology
NCCITS	NASA Competency Center for Information Technology Security
NPD	NASA Policy Directive
NPG	NASA Procedures and Guideline
NRP	NASA Resource Protection
NSA	National Security Agency

O

ODIN	Outsource Desktop Initiative NASA
OIG	Office of the Inspector General
OMB	Office of Management and Budget

P

PAO	Public Affairs Office
PC	Personal computer
PCITS	Principal Center for Information Technology Security
PL	Public Law
PKI	Public Key Infrastructure
PUB	Public Access

R

RA	Registration Authority
RFP	Request for Proposal

S

SA	System Administrator
SEB	Source Evaluation Board
SER	Scientific, Engineering, and Research
SMA	Special Management Attention
SOLAR	NASA Site for On-Line Learning and Resources
SOW	Statement of Work

T

TCP	Transmission Control Protocol
T-POC	Technical Point of Contact

U

U.S.C.	United States Code

V

VPN	Virtual Private Network

W

WFF	Wallops Flight Facility
WSC	White Sands Complex

Appendix B – Index

This index uses paragraph numbers instead of page numbers.

APPENDIX C – Remediation Process for Compromised Systems

A. Procedures for Reconnecting a Compromised Windows NT System

THE FOLLOWING PROCEDURES MUST BE COMPLETED BEFORE A REQUEST TO RECONNECT A COMPROMISED WINDOWS NT SYSTEM CAN BE SUBMITTED.

1. Setting up the machine.
   - Reformat the Hard drive and re-install the operating system from the original media. **Do not use a backup tape to re-install the system.**
   - Physically secure the server.
   - Protect the system from undesirable booting.
   - Install all security patches.
   - Disable all unused services.
   - Install an Access Warning Banner on the system. Attach a copy of the banner to the Executive Summary (See step 10.)

2. Establish strong password controls and secure account policies.
   - Change root password(s).
   - Change all vendor default passwords.
   - Lockout attempts to gain access after these attempts and make passwords hard to guess.

   (All passwords must meet the requirements of NPG 2810.1, paragraphs A.6.3.2 d A.6.3.3.)
   - Enable Administrator account lockout and rename the Administrator account.
   - Establish separate accounts for Administrators.
   - Set up an Administrator password control process.
   - Secure and manage event logs.
   - Run an ACL reporting tool.
   - Encrypt SAM'S password database with 128-bit encryption.

3. Setting registry keys
   - Avoid the Netware DLL Trojan Horse (contact Center IT Security Manager (ITSM) for additional information).
   - Secure print drivers.
   - Restrict anonymous logon.
   - Control remote access to the Registry.
   - Restrict anonymous network access to Registry and to look up account names, groups and shares.
   - Control access to the command scheduler.
   - Secure the Registry.
   - Block the 8.3 attack (contact ITSM for additional information).

4. Auditing
   - Turn on auditing.
   - Monitor the audit logs.

5. Networking and internet security settings
   - Turn off all unneeded network services and run needed services safely.
   - If you use Internet Information (IIS), block known vulnerabilities.
   - Protect vulnerable ports through screening router.

6. Other actions required as the system is set up
   - Require password-protected screen saver on all workstations.
   - Implement virus protection software.
   - Check for and remove ROLLBACK.

7. Verify that the IP address is registered properly in the CNE IP database.

8. Scan the reinstalled operating system to ensure that all vulnerabilities have been corrected. (This will be a full ISS scan; once the scan is performed all vulnerabilities will have to be fixed.)
   - Access to the GITSVST Secure Server is limited to organizational CSO's and directorate CSO's.
   - https://wurtzberg.gsfc.nasa.gov/ and Procedures for Requesting Keys for an ISS Scan.
   - Follow the link in the left frame to Internet Scanner Files to download the latest Certification Scanning policy.

9. Prepare an IT Security Incident Report (WS Word, 21KB). Submit a copy to the ITSM.

10. The DCSO will submit a Security Plan with an Executive Summary "documenting the steps taken to fix all vulnerabilities" along with an "Authorization to Process" with a "Division-Level" signature (See NPG 2810.1, paragraph A.6.12) to the ITSM.

Off-Site Compromised Systems

Compromised systems located at an off-site contractor facility must also complete the following actions.

11. Prepare a justification that addresses the following issues.
   - Why does this system need gsfc.nasa.gov DNS names?
   - Why does this system need a direct connection to GSFC?
   - Why can't the contractor utilize a Wide Area Network (WAN) style connection instead of the current Metropolitan Area Network (MAN) style connection?

12. The DCSO and the Division Chief of the responsible GSFC organization must sign the justification.

B. Procedures for Reconnecting a Compromised UNIX System

The following procedures must be completed before a request to reconnect a compromised system can be submitted.

1. Reformat the Hard drive and re-install the operating system from the original media.
   - **Do not use a backup tape to re-install the system.**

2. Change root password(s).
   - Ensure that all user passwords are also changed.
   - Since users tend to re-use passwords, it is also strongly recommended that users change passwords on any other machines on the local network.
   - Ensure that this root password is not also used on other machines.
   - **All passwords must meet the requirements of NPG 2810.1, paragraphs A.6.3.2 and A.6.3.3**

3. Change all vendor default passwords.
   - Disable all unused accounts.

4. Install all security patches.
   - Importantly: Install patches for mounted and BIND/named.

5. Disable all unused services.
   - Disable all Rhosts based services if at all possible.
   - Disable telnet and use SSH instead if at all possible.
   - Likewise disable FTP and use SCP if at all possible.

6. Install an Access Warning Banner on the system.
   - Specify which services have had the warning banner implemented. In particular SSH, Telnet (if used), ftp (if used) at a minimum.
   - Attach a copy of the banner to the Executive Summary (See step 14).

7. Verify that the IP address is registered properly in the CNE IP Database.

8. Scan the reinstalled operating system to ensure that all vulnerabilities have been corrected. (This will be a full ISS scan; once the scan is performed all vulnerabilities will have to be fixed.)
   - Access to the GITSVST Secure Server is limited to organizational CSO's and directorate CSO's.
   - https://wurtzberg.gsfc.nasa.gov/ and Procedures for Requesting Keys for an ISS Scan.
   - Follow the link in the left frame to Internet Scanner Files to download the latest Certification Scanning policy.

9. Install TCP Wrappers (Information can be obtained by visiting NASIRC web site: http://www-nasirc.nasa.gov/nasa/ -- click on "Services" and then "Toolkits".)
   - Ensure that all possible tcp and udp services that allow external connections that can be protected by tcp-wrappers are indeed wrapped.
   - Ensure that the allowed external connections to the machine are the minimum possible and that the system "trusts" the fewest number of other systems that it can and still perform its required function.

10. Install ssh (download free version from http://www.openssh.org/).
   - Ensure at a minimum that root uses ssh if not all the users of the system.

11. Install Tripwire (Information can be obtained by visiting NASIRC web site http://www-nasirc.nasa.gov/nasa/ -- click on "Services" and then "Toolkits".)
   - Conduct a critical file audit of the system, and enter all security sensitive data files and executables into the tripwire database.
   - Ensure that tripwire is run frequently (at least once per day) to verify the files' integrity.

12. Prepare a Log Host Review.
   - Implement or utilize an external loghost capability that will ensure that system logs are sent to an external machine and regularly reviewed.

13. Prepare an IT Security Incident Report (WS Word, 21KB). Submit a copy to the Center IT Security Manager.

14. The DCSO will submit a Security Plan with an Executive Summary "documenting the steps taken to fix all vulnerabilities" along with an "Authorization to Process" with a "Division Level signature (See NPG 2810.1, paragraph A.6.12) to the Center IT Security Manager.

Off-Site Compromised Systems

Compromised systems located at an off-site contractor location must also complete the following actions.

15. Prepare a justification that addresses the following issues.
   - Why does this system need gsfc.nasa.gov DNS names?
   - Why does this system need a direct connection to GSFC?
   - Why can't the contractor utilize a Wide Area Network (WAN) style connection instead of the current Metropolitan Area Network (MAN) style connection?

16. The DCSO and the Division Chief of the responsible GSFC organization must sign the justification.

APPENDIX D – REPORTING AN IT SECURITY INCIDENT

System/Network User

The System/Network User is responsible for

Reporting all suspected and actual incidents to your system/network administrator and your organizational management.

Note: Do not disconnect the system from the network unless directed by the CSO, DCSO, or Center/Deputy Center IT Security Manager: keeping the network connection can possibly help determine the source of an incident.

System/Network Administrator

The System/Network Administrator is responsible for:

1. Preparing and submitting a written incident report to the CSO.
2. Assisting in the investigation of IT security incidents.
3. Repairing any damage done to the system/network operating system.

Organizational Computer Security Official (CSO)

The Organizational CSO is responsible for:

1. Reporting actual or suspected IT security incidents to the Center/Deputy Center ITSM.
2. Notifying organization and contractor management of any incident involving IT resources under their control.
3. Submitting a written incident report to the Center/Deputy Center ITSM.
4. Maintaining a file of IT security incident reports.

Center/Deputy Center IT Security Manager (ITSM)

The Center/Deputy Center It Security Manager is responsible for:

1. Responding to IT security incidents and ensuring that they are handled according to the guidance in NASA Procedures and Guidelines (NPG) 2810.1
2. Notifying the Center Chief Information Officer (CIO) and the NASA Incident Response Center (NASIRC) of IT security incidents.
3. Reporting all incidents that may constitute a computer crime to the Office of the Inspector General (OIG).

APPENDIX E – INCIDENT REPORT

GENERAL

a. Submitted By**:**
b. Date of Report**:**

SYSTEM INFORMATION

a. System/IP Address:
b. Location: (Bldg/room/offsite location)
c. Hardware/OS:
**d. Category of information processed:
e. Is logon warning banner installed?

CONTACT PERSON FOR IT RESOURCE AFFECTED

a. Name/Telephone #:
b. Org Code/Contractor name:
c. Email Address:

DESCRIPTION OF INCIDENT

a. What occurred?
b. Date & Time of Incident:
c. How was the incident discovered?
d. IP Address of Hostile Site:

COST TO CLEANUP/REPAIR SYSTEM

a. Damage caused by incident:
b. Man hours spent to cleanup/repair:

INCIDENT REPORTED TO:

****

**** CATEGORIES OF INFORMATION (Per NPG 2810.1, Paragraph 4.2.9)**

MSN - Mission Information
BSR - Business and Restricted Technology Information
SER - Scientific, Engineering, and Research Information
ADM - Administrative Information
PUB - Public Access Information

APPENDIX F – Center Mail Relay Registration Policy

GSFC Computer Systems electronic mail (email) relay services shall be controlled.

APPROVAL:

Line Managers shall approve the configuration of GSFC computer systems to enable email relay services and shall register the activation of those services with the Information Services and Advanced Technology Division (Code 290) through the CNE web site.

It is understood that line manager approval authority shall be at or as close to the first line of supervision or group/task leadership as is determined by the home organization to be appropriate.

EFFECTIVE DATE:

This policy is effective immediately.

Registration of GSFC computer system email relay services with Code 290 through the CNE web site shall be completed within 30 days of release of this policy.

There are two ways to access the registration page.

Go to the CNE web site, http://cne.gsfc.nasa.gov/, select "Email Services", and then select "Mail Relay Service Registration" from the "Email Services" menu.

Or, use the URL http://cne.gsfc.nasa.gov/Mail_Relay_Service_Register that pulls up the form links directly.

BACKGROUND:

GSFC is routinely enabling "spam email" by third parties because it does not effectively manage or control its mail relay services. GSFC has been notified innumerable times by outside entities that tens of thousands of inappropriate email messages have been sent by a third party to Internet destinations, relayed unknowingly through GSFC computer systems. In the interest of our civic duties, improved security, and to help ensure that GSFC computing assets are applied to business purposes, GSFC must assume better responsibility for managing its email services.

Further, many GSFC systems are currently configured by default to receive email, but most of these systems are not intended to be mail servers. For those systems not intentionally functioning as email servers, the system should not accept any email for delivery. This is a simple configuration change. By default most systems (e.g.UNIX) are configured to accept Internet email. The Simple Mail Transport Protocol (SMTP) process runs on "tcp port 25" and will attempt to deliver any messages it receives, to include spam email. Most GSFC systems do not require the capability to receive email, and should be configured appropriately.

Technical background information is also available at the System Administration, Networking, and Security Institute (SANS) web site; for example, see the following frequently asked questions (FAQ):

http://www.sans.org/infosecFAQ/email/open_relay.htm

An excerpt from that FAQ is provided here:

" What is third party mail relay or open relay"?

It is the ability of an email server to receive email from an unknown sender and then sending it on to a recipient or recipients, which could number in the thousands, that are not users of that email system.

The protocol responsible for relaying is called SMTP or Simple Mail Transfer Protocol. This protocol belongs to the TCP/IP family and is used by email servers to transfer email from the senders email server to the recipient or recipients' email server or servers. The default port that it works on is port 25.

The sole responsibility of SMTP is to relay email from the host to the recipient's email server. It is the responsibility of the email administrator to restrict this relaying function so that it is not an open relay, but a controlled relay. This is done in different ways depending on the email server platform. To get a detailed explanation of the SMTP protocol and how it works see the Internet Engineering Task Force's (IETF) Request for Comments (RFC) 821 and 822 located at http://www.ietf.org "

Direct questions to the Center/Deputy Center IT Security Manager or your Directorate or Organizational Computer Security Officials (CSOs). See http://forbin2.gsfc.nasa.gov/297/services/dcso/dcso.stm for a list of GSFC DCSO/CSOs.

APPENDIX G - CENTER ACCOUNT REQUEST DOCUMENT

INSTRUCTIONS FOR COMPLETION OF ACCOUNT REQUEST DOCUMENT

1. An Account Request Document required for each user who requests access to a multi-user IT system.

2. Affiliation - organization code, company name, university name, or other affiliation identification.

3. If not a US citizen, indicate citizenship status, such as Permanent Resident Alien or Foreign National. If not accessing the system from within the United States, indicate from what country normal access will occur.

4. For non-Government employees, identification of the official relationship of the requester to NASA (e.g., grant, Memorandum of Understanding, contract, or other work agreement).

5. Access Levels of user – Privileged, Limited privileged, Non-privileged. Foreign nationals who are not international partners cannot be granted **privileged** or **limited privileged** access.

6. A Government management official's signature, such as a Branch Chief, Resource Monitor, Grant Monitor, data owner, or Contracting Officer's Technical Representative (COTR), who approves the legitimate need to access the systems to perform, authorized Government activities. A Government designee may be appointed to sign in place of the Government management official.

ACCOUNT REQUEST DOCUMENT

_____ _____ _____
Last Name First Name Middle Initial

_____
Mailing Address

_____ _____
Telephone Number Email Address

_____
Affiliation

_____
Citizenship of the Requester

_____
System, or group of systems, for which an account is being requested

_____
Level of user privileges afforded to the account

Acknowledgement Statement

Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Section 799, Title 18, U.S. Code; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts, and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

_____ _____
Requester's Signature Date Signed

APPROVED BY:

Name_____

Title_____ Org Code_____

CHANGE HISTORY LOG

Revision	Effective Date	Description of Changes
Baseline	04/16/03	Initial Release